# Figure 1
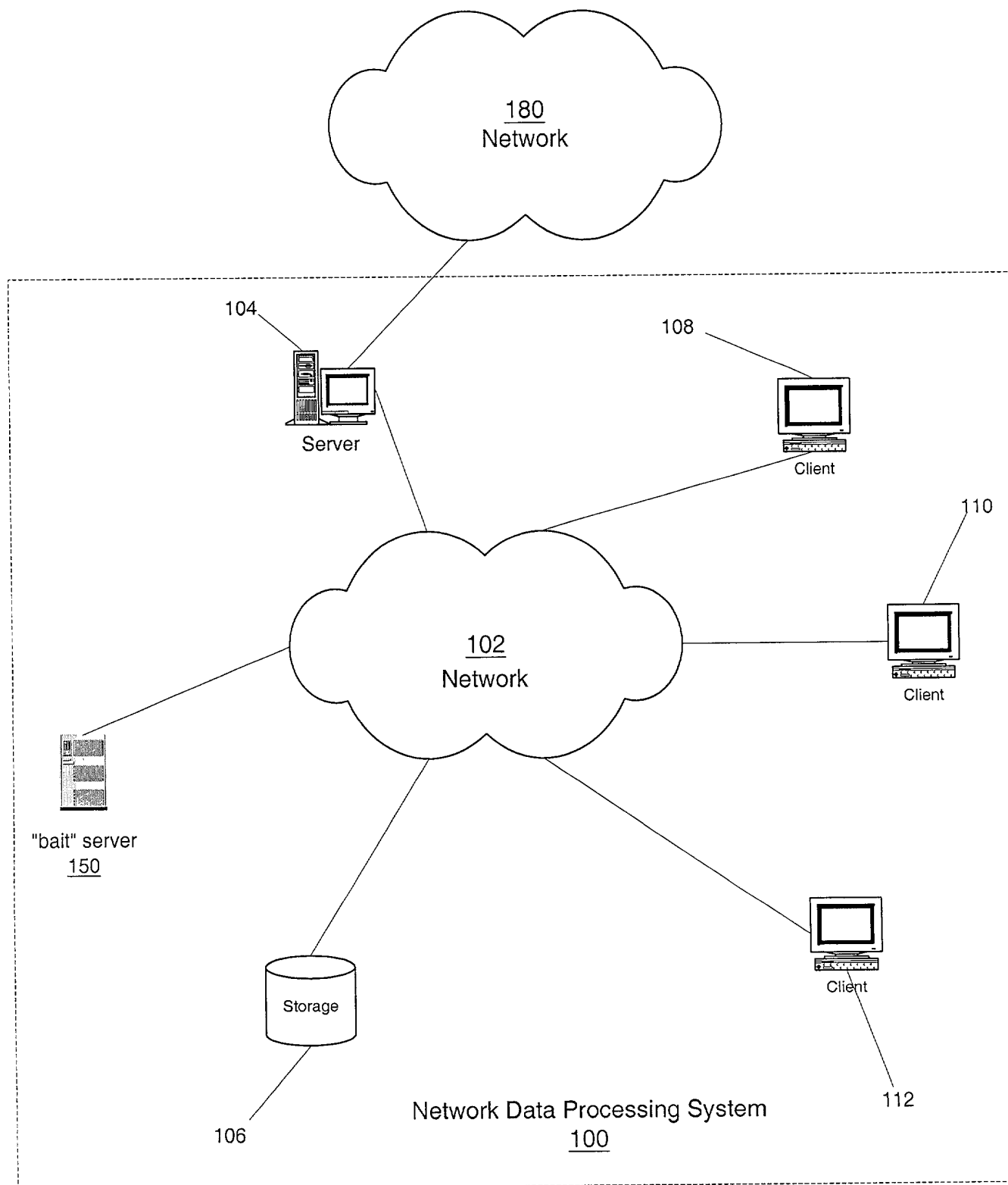
Chefalas et al.
YOR920010015US1
Method and Apparatus for the Detection, Notification,
and Elimination of Certain Computer Viruses on a
Network Using a Promiscuous System as Bait
Page 1 of 5

180
Network

104

108

Server

Client

110

102
Network

Client

"bait" server
150

Client

Storage

Network Data Processing System
100

106

112

# Figure 2

# Figure 3

Processor
302

Host/PCI
Cache/Bridge
308

Main Memory
304

Audio
Adapter
316

Bus      306

SCSI
Host Bus
Adapter
312

LAN
Adapter
310

Expansion Bus
Interface
314

Graphics
Adapter
318

Audio/Video
Adapter
319

Disk
326

Tape
328

CD-
ROM
330

300

Keyboard
and Mouse
Adapter
320

Modem
322

Memory
324

332

# Figure 4

Chefalas et al.
YOR920010015US1
Method and Apparatus for the Detection, Notification,
and Elimination of Certain Computer Viruses on a
Network Using a Promiscuous System as Bait
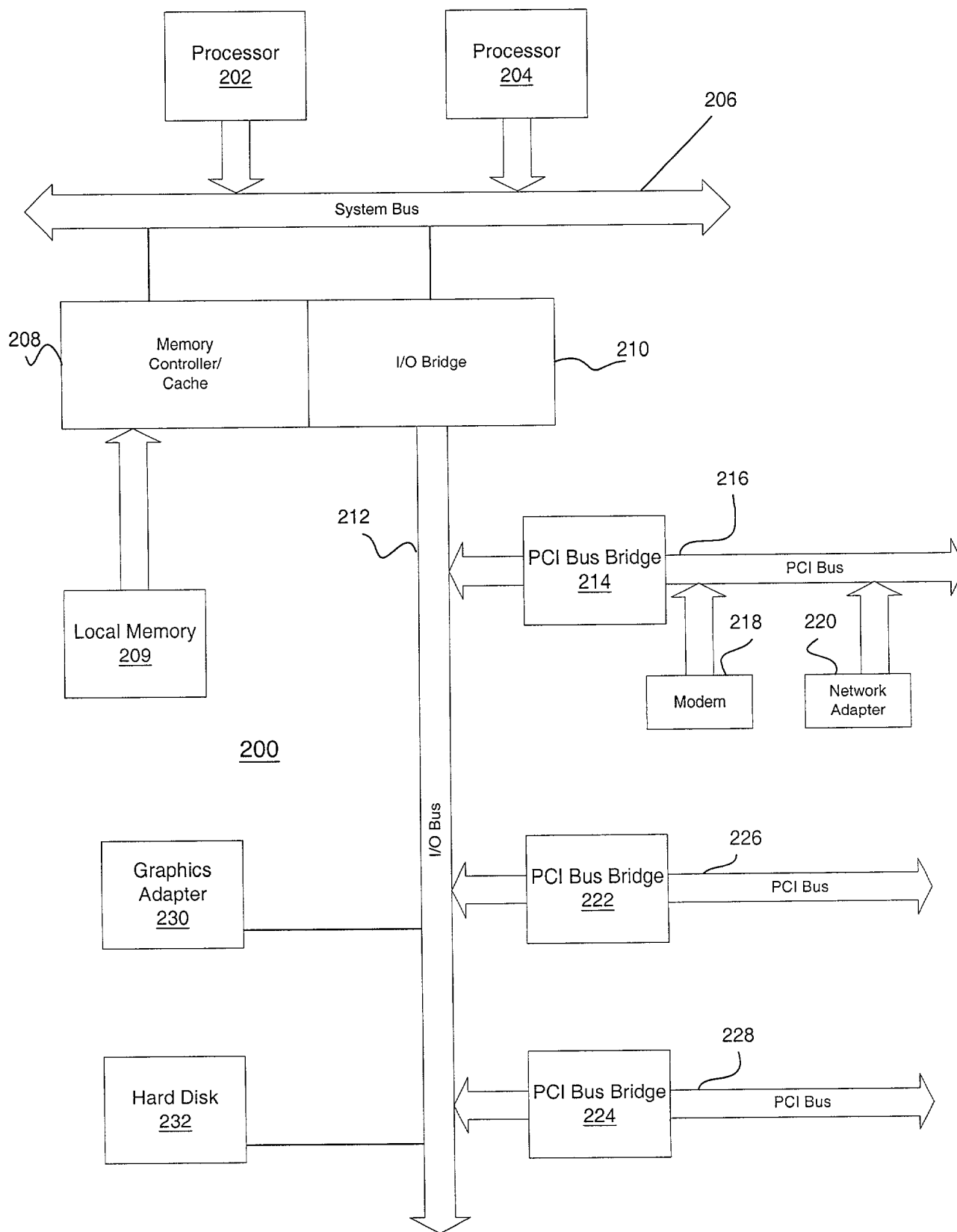Page 4 of 5

400

```
                        ( Start )
                           |
                           v
              +----------------------------+
              |        Power on.           |
              |          402               |
              +----------------------------+
                           |
                           v
              +----------------------------+
              | Normal operation with      |
              | virus monitoring.          |
              |          404               |
              +----------------------------+
                           |
                           v
                      /  Power   \
                     < off event? >---YES--->( Finish )
                      \   406    /
                           |
                          NO
                           |
                           v
                      /  Virus   \
                     <  event?   >
                      \   408    /
                           |
                          YES
                           |
                           v
              +----------------------------+
              | Identify offending computer|
              | and send notification to   |
              | remote administrator.      |
              |          410               |
              +----------------------------+
                           |
                           v
              +----------------------------+
              | Remove connections and     |
              | shares for offending       |
              | computer.                  |
              |          412               |
              +----------------------------+
                           |
                           v
              +----------------------------+
              | Instruct offending computer|
              | to disinfect itself.       |
              |          414               |
              +----------------------------+
                           |
                           v
              +----------------------------+
              | Wait for reconnect request.|
              |          416               |
              +----------------------------+
                           |
                           v
                      / Reconnect  \
       +--YES--------< request       >---NO---+
       |              \ received? 418/        |
       v                                      (back to 416)
+------------------------+
| Reconnect offending    |
| computer.              |
|        420             |
+------------------------+
```
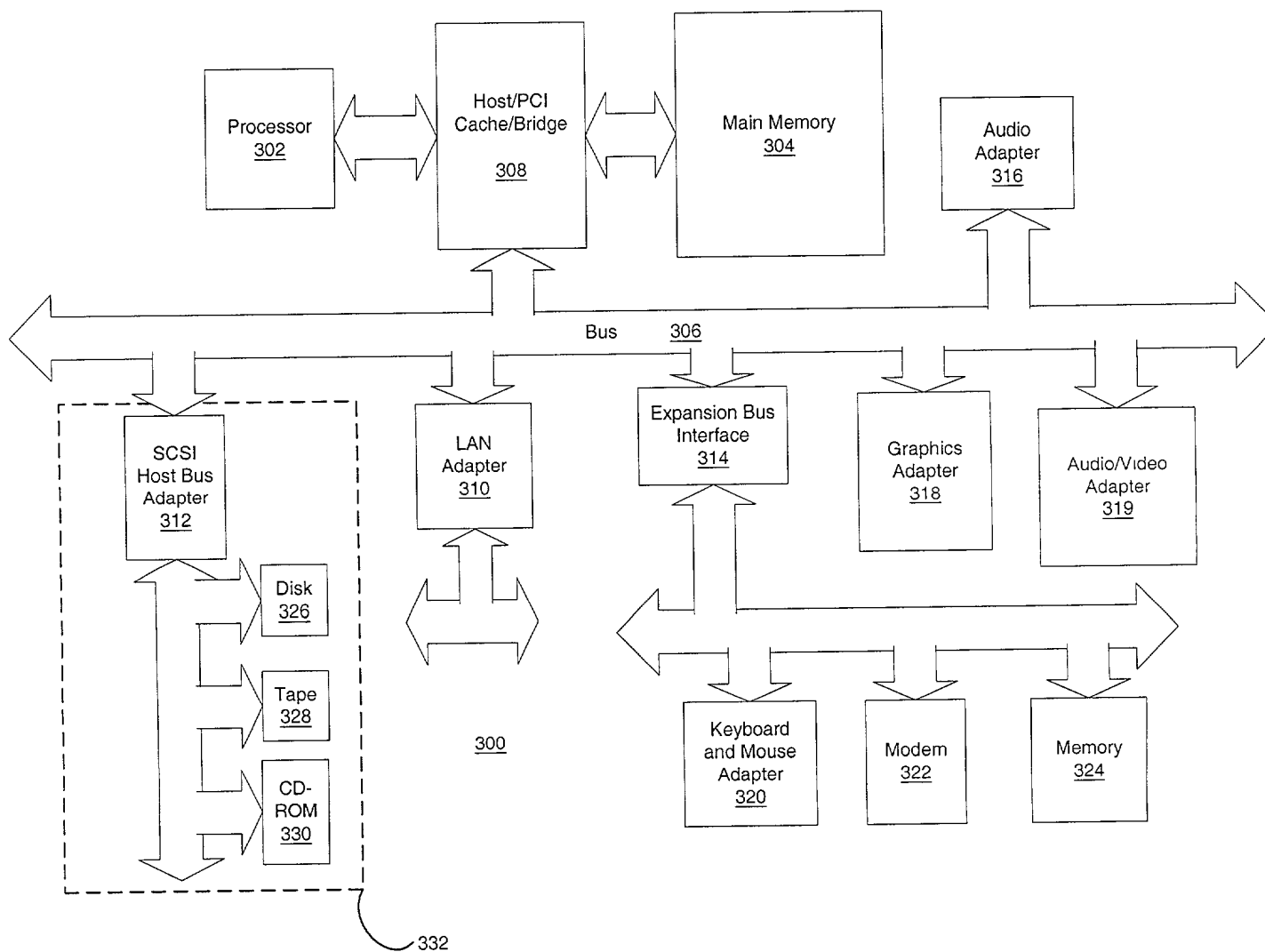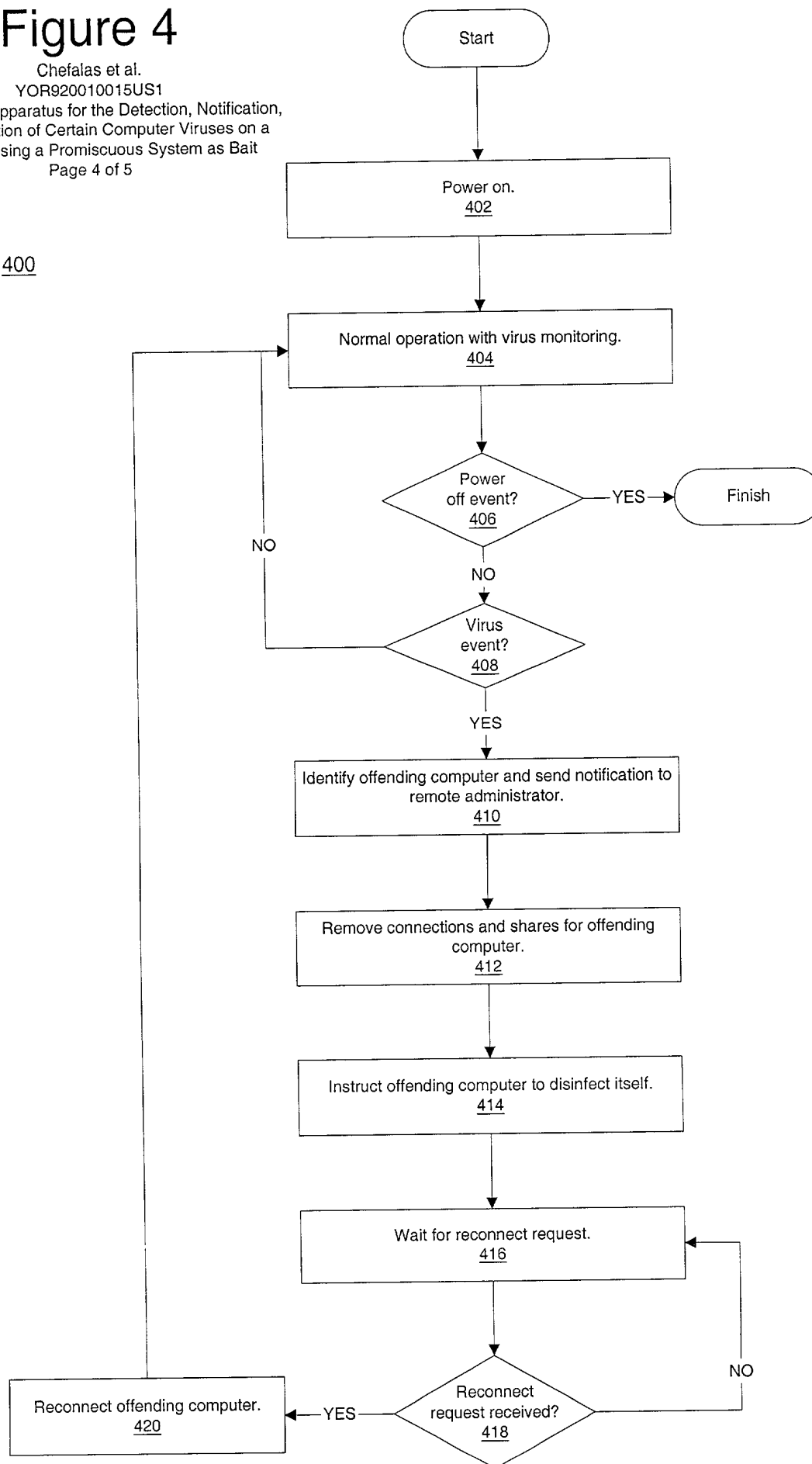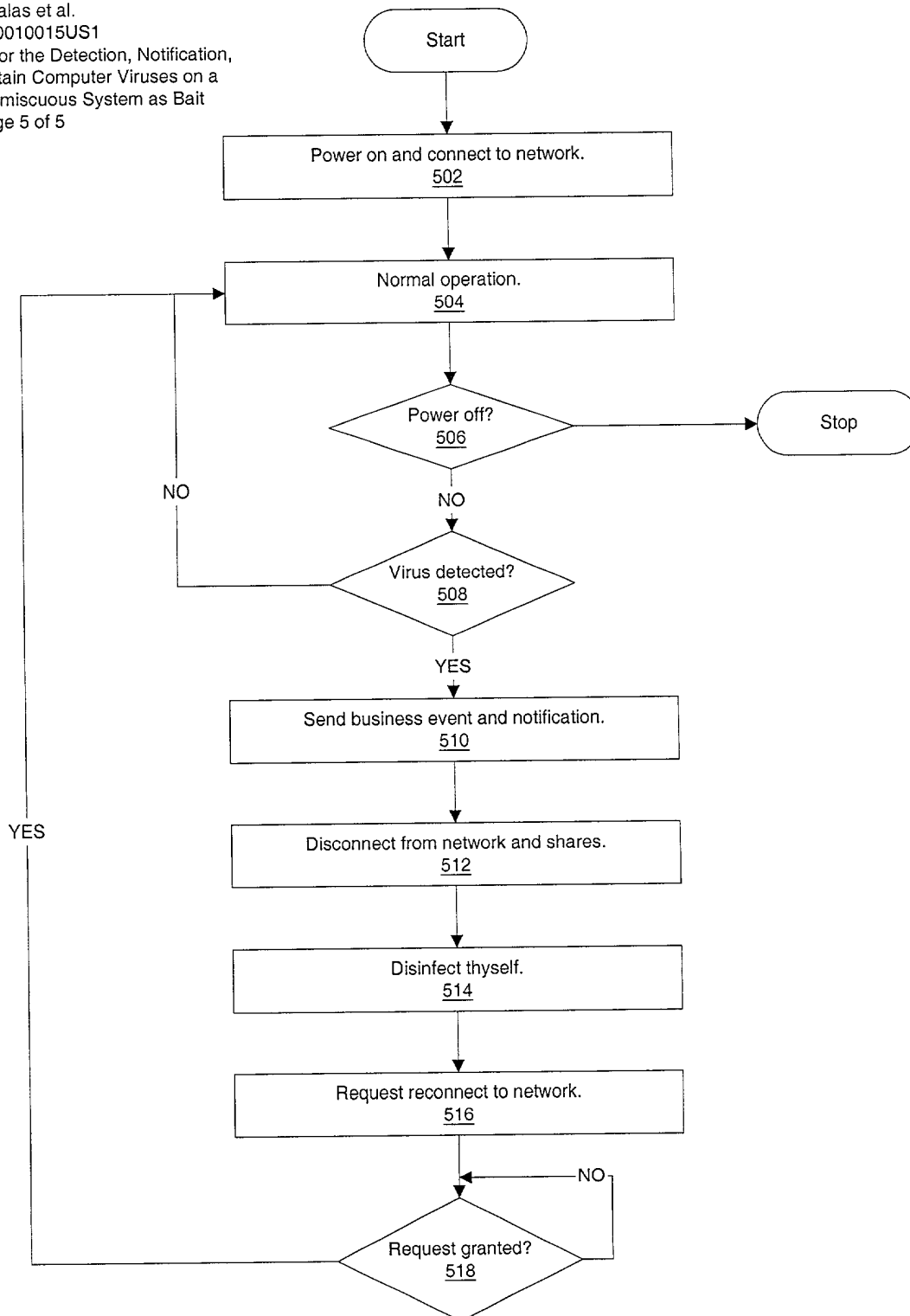
Server operation

# Figure 5

Chefalas et al.
YOR920010015US1
Method and Apparatus for the Detection, Notification,
and Elimination of Certain Computer Viruses on a
Network Using a Promiscuous System as Bait
Page 5 of 5

```
                              ( Start )
                                 │
                                 ▼
              ┌──────────────────────────────────────┐
              │   Power on and connect to network.   │
              │                502                   │
              └──────────────────────────────────────┘
                                 │
                                 ▼
      ┌──────────────────────────────────────┐
   ┌─▶│           Normal operation.          │
   │  │                504                   │
   │  └──────────────────────────────────────┘
   │                         │
   │                         ▼
   │                    ◇ Power off?  ◇──────────────▶ ( Stop )
   │                    ◇    506     ◇
   │             NO          │
   │                         │ NO
   │                         ▼
   │                    ◇ Virus detected? ◇
   │◀───────────────────◇      508        ◇
   │    NO                   │
   │                         │ YES
   │                         ▼
   │  ┌──────────────────────────────────────┐
   │  │  Send business event and notification.│
   │  │                510                   │
   │  └──────────────────────────────────────┘
   │                         │
   │                         ▼
   │  ┌──────────────────────────────────────┐
   │  │    Disconnect from network and shares.│
   │  │                512                   │
   │  └──────────────────────────────────────┘
   │                         │
   │                         ▼
   │  ┌──────────────────────────────────────┐
   │  │          Disinfect thyself.           │
   │  │                514                   │
   │  └──────────────────────────────────────┘
   │                         │
   │                         ▼
   │  ┌──────────────────────────────────────┐
   │  │     Request reconnect to network.     │
   │  │                516                   │
   │  └──────────────────────────────────────┘
   │                         │
   │                         ▼       ──NO─┐
   │                    ◇ Request granted? ◇◀─┘
   │ YES                ◇      518        ◇
   └────────────────────◇                ◇
```

Client operation

500